JULY 2014

End of Support for Microsoft Windows XP & Microsoft Office 2003

Introduction

1. The Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Intrusions* ranks timely patching of applications and operating systems as the second and third most effective strategies to mitigate targeted cyber intrusions.

2. In April 2014, Microsoft ended support for Microsoft Windows XP and Microsoft Office 2003. Organisations yet to upgrade from this software should review their threat and risk assessments for their ICT environments and implement additional controls to reduce their risk exposure.

Intended audience

3. This advice is intended for organisations still operating Microsoft Windows XP and/or Microsoft Office 2003.

Scope

4. This document is separated into:

   a. mitigation strategies for organisations operating an entire Microsoft Windows XP and Microsoft Office 2003 fleet

   b. mitigation strategies for organisations that have limited remaining Microsoft Windows XP and Microsoft Office 2003 deployments to support legacy business applications.

Operating an entire fleet

5. Organisations continuing to operate an entire Microsoft Windows XP and Microsoft Office 2003 fleet should implement the following host-based controls:

   a. **Mitigation Strategy #1:** Implement an application whitelisting solution, such as Software Restriction Policies (SRP). Application whitelisting, when implemented appropriately, can detect and prevent malicious code execution, network propagation and data exfiltration by an adversary.

b. **Mitigation Strategies #2 and #3:** Negotiate an extended support arrangement with Microsoft for the provision of patches for security vulnerabilities in Microsoft Windows XP, Microsoft Office 2003 and Internet Explorer. Whilst an extended support arrangement won't address all security vulnerabilities disclosed for legacy Microsoft applications, it will reduce the attack surface of workstations.

c. **Mitigation Strategies #2, #5 and #29:** For unsupported applications (e.g. Microsoft Office 2003 and Internet Explorer 8) either upgrade to supported versions, or if this is not possible, consider removing the application, using alternative applications to achieve similar business functionality or enabling in-built application features such as Office File Validation and Protected View for Microsoft Office. Each application upgraded, removed or replaced with an alternative generally reduces the attack surface of workstations and can assist in preventing malicious code execution.

d. **Mitigation Strategies #4 and #9:** Ensure that privileged account credentials are not entered into Microsoft Windows XP workstations e.g. to administer the workstation or other applications or systems within an organisation's ICT environment. Instead, a vendor-supported operating system should be used for these activities, and a low privileged account used for all other non-administrative activities. Microsoft Windows XP workstations are at a higher risk of being compromised due to unpatched vulnerabilities, and lack additional security functionality of newer Microsoft Windows versions to protect privileged account credentials from being captured by an adversary and used to propagate throughout a network.

e. **Mitigation Strategy #7:** Implement Microsoft's Enhanced Mitigation Experience Toolkit (EMET) on workstations. Implementing EMET for applications that commonly interact with data from untrusted sources (e.g. Adobe Reader, Adobe Flash, Oracle Java, Microsoft Internet Explorer and Microsoft Office) can reduce the risk of successful malicious code execution as well as assisting in the identification of such attempts.

f. **Mitigation Strategies #21, #25 and #27:** Apply basic hardening, where possible, to workstations and user accounts. Applying basic hardening principles to workstations, such as disabling unneeded functionality or common intrusion vectors such as autorun, SMB and NetBIOS services, can assist in preventing malicious code execution and network propagation by an adversary.

g. **Mitigation Strategies #12 and #13:** Implement a third party software-based application firewall on workstations that performs both inbound and outbound filtering of traffic. A software-based application firewall can assist in detecting and preventing malicious code execution, network propagation and data exfiltration by an adversary.

h. **Mitigation Strategies #22 and #30:** Ensure antivirus applications on workstations continue to be supported by vendors. If support ceases from a vendor, switch to an alternative vendor that

continues to offer Microsoft Windows XP support. The use of antivirus applications on workstations can assist in detecting and preventing malicious code execution.

6. In addition to the above host-based controls, the following controls can be implemented to reduce the likelihood of malicious code reaching workstations in the first place. These include:

a. **Mitigation Strategy #6:** Implement automated dynamic analysis of email and web content in a sandbox to detect suspicious behaviour. By analysing data from untrusted sources for suspicious activity upon simulated user interaction, malicious code can be identified and blocked from reaching vulnerable workstations.

b. **Mitigation Strategies #I7 and #18:** Implement email and web content filtering of incoming and outgoing data to only allow approved file types. By controlling the types of data that reach workstations, organisations can reduce the likelihood of malicious code execution and as well as identifying the source of any such attempts.

c. **Mitigation Strategy #26:** Prevent users from connecting portable media to workstations. Portable media infected with malicious code can result in the exploitation of vulnerable workstations. As Microsoft Windows XP workstations are more susceptible to exploitation, data transfers to such workstations should be controlled via an organisation's ICT service desk to reduce the likelihood of malicious code execution and data exfiltration.

Operating a limited deployment

7. Organisations continuing to operate a limited Microsoft Windows XP and Microsoft Office 2003 deployment to support legacy business applications should consider implementing the following controls:

a. **Mitigation Strategy #10:** Isolate Microsoft Windows XP workstations from other workstations and non-essential network services. This can reduce the risk of an adversary using a compromised Microsoft Windows XP workstation to propagate throughout a network and access other network resources.

b. **Mitigation Strategy #14:** Virtualise access to Microsoft Windows XP operating environments and required applications from within a vendor-supported operating system e.g. Microsoft Windows 7. Using virtualised environments can hamper an adversary's ability to extend their reach beyond the virtualised environment and propagate to other network resources.

c. **Mitigation Strategy #23:** Deny access from Microsoft Windows XP workstations to the Internet. As legacy business applications are likely to operate in a local stand-alone mode, or only require access over an organisation's intranet, restricting access from such workstations to the Internet can reduce the risk of data exfiltration by an adversary should they ever became compromised.

Additional considerations

8. Independent of how Microsoft Windows XP and Microsoft Office 2003 are operated by organisations, additional controls can be implemented to assist in the identification and remediation of cyber intrusions. These include:

a. **Mitigation Strategies #15 and #16:** Implement a robust centralised logging and auditing framework to capture and analyse both computer and network-based events. An appropriate auditing framework within an organisation can assist in identifying individual workstations that may have been compromised as well as helping to tailor incident response measures to remove infected workstations from an organisation's network.

Further information

9. This document complements the advice listed in ASD's *Strategies to Mitigate Targeted Cyber Intrusions.* This publication is available at http://www.asd.gov.au.

10. Further information on patching applications and operating systems can be found in ASD's Protect publication *Assessing Security Vulnerabilities and Patches*. This document, and additional ASD Protect publications, can be found at http://www.asd.gov.au/publications/index.htm.

Contact details

Australian Government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.